IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) An apparatus for encrypting block data of a first size comprising:

encrypting sections connected in series, each of the encrypting sections comprising,

first units each configured to randomize first subblock data of a second size which are obtained by dividing the block data of the first size, and

a second unit configured to diffuse a group of data which is of the first size and is output from the first units ~~with respect to the first size~~ and supply a result of diffusion to first units in a succeeding encrypting section, and wherein the first units and the second unit are configured to connect at least one input bit terminal of the first units to one input bit terminal of the corresponding first unit in the succeeding encrypting section via at least two paths.

2 (Canceled).

3 (Canceled).

4. (Currently Amended) An apparatus for encrypting block data of a first size, the apparatus comprising:

encrypting sections connected in series, each of the encrypting sections comprising,

first nonlinear transformation units each configured to perform a nonlinear transformation process for first subblock data of a second size which are obtained by dividing the block data of the first size, and

a first linear diffusion unit configured to perform a linear diffusion process for a group of the first subblock data which is of the first size and is output from the first nonlinear transformation units ~~with respect to the first size~~ and supply a result of the linear diffusion process to first nonlinear transformation units in a succeeding encrypting section,

wherein each of the first nonlinear transformation units comprises,

second nonlinear transformation units each configured to perform a nonlinear transformation process for second subblock data of a third size which are obtained by dividing the first subblock data of the second size, and

a second linear diffusion unit configured to perform a linear diffusion process for a group of the second subblock data which is of the third size and is output from the second nonlinear transformation units~~ with respect to the second size~~, and

wherein the first nonlinear transformation units, the first linear diffusion unit, the second nonlinear transformation units, and the second linear diffusion unit are configured to connect at least one input bit terminal of the first nonlinear transformation units to one input bit terminal of the corresponding first nonlinear transformation units in the succeeding encrypting section via at least two paths.

5. (Previously Presented) The apparatus according to claim 4, wherein

input bit terminals of a second non-linear transformation unit are connected to input bit terminals of a corresponding second nonlinear transformation unit in the succeeding first nonlinear transformation unit via at least two paths.

6. (Previously Presented) The apparatus according to claim 4, wherein

input bit terminals of more than one of the second nonlinear transformation units are connected to input bit terminals of corresponding second nonlinear transformation units in the succeeding first nonlinear transformation unit via at least two paths.

7 (Canceled).

8. (Previously Presented) The apparatus according to claim 4, wherein the block data is 128 bits in length, each of the first subblock data is 32 bits in length.

9. (Original) The apparatus according to claim 4, wherein the first linear diffusion unit is implemented by hardware.

10. (Previously Presented) The apparatus according to claim 9, wherein an input-output characteristic of the first linear diffusion unit is based on multiplication in a Galois field.

11. (Original) The apparatus according to claim 5, wherein the first linear diffusion unit is implemented by software.

12. (Currently Amended) An apparatus for encrypting block data of 128 bits, the apparatus comprising:

encrypting sections connected in series, each of the encrypting sections including,

four first nonlinear transformation units each configured to perform a nonlinear transformation process for first subblock data of 32 bits which are obtained by dividing the block data, and

a first linear diffusion unit configured to perform a linear diffusion process using a maximum distance separable matrix for a group of the first subblock data of 128 bits output from the four first nonlinear transformation units ~~with respect to the first size~~ and supply a result of the linear diffusion process to four first nonlinear transformation units in a succeeding encrypting section;

a key addition unit which adds key data of 128 bits to output data of 128 bits from the encrypting section of ~~the~~ a last stage, wherein an encrypting section of [[a]] the last stage comprises four nonlinear transformation units each configured to perform a nonlinear transformation process for the first subblock data of 32 bits,

wherein each of the first nonlinear transformation units includes stage sections, each stage section including,

four second nonlinear transformation units each configured to perform a nonlinear transformation process for second subblock data of 8 bits which are obtained by dividing the first subblock data,

a second linear diffusion unit configured to perform a linear diffusion process for a group of the second subblock data of 32 bits output from the second nonlinear transformation units~~ with respect to the second size~~, and

an adder for adding a key to four second subblock data of 8 bits input to the four second nonlinear transformation units,

wherein a stage section of [[a]] the last stage comprises four second nonlinear transformation units each configured to perform a nonlinear transformation process for the second subblock data;

wherein the first nonlinear transformation units, the first linear diffusion unit, the second nonlinear transformation units, and the second linear diffusion unit are configured to connect at least one input bit terminal of the first nonlinear transformation units to one input bit terminal of the corresponding first nonlinear transformation units in the succeeding encrypting section via at least two paths, and

wherein each of the four first nonlinear transformation units divides input data of 32 bits into eight groups of data of 4 bits which are formed of extracting the input data by every 8 bits, and the first linear diffusion unit comprises eight subunits each subunit receiving corresponding four groups of data of 4 bits output from the four first nonlinear transformation units, performing a 4 × 4 matrix operation based on multiplication over a Galois field GF(2^4) for the received four groups of data of 4 bits, and outputting four groups of data of 4 bits to corresponding four first nonlinear transformation units ~~(103)~~ of the succeeding encrypting section.

13. (Currently Amended) An apparatus for encrypting block data of 64 bits, the apparatus comprising:

encrypting sections connected in series, each of the encrypting sections including, two first nonlinear transformation units each configured to perform a nonlinear transformation process for first subblock data of 32 bits which are obtained by dividing the block data, and

a first linear diffusion unit configured to perform a linear diffusion process using a maximum distance separable matrix for a group of the first subblock data of 64 bits output from the ~~four~~ two first nonlinear transformation units ~~with respect to the first size~~ and supply a result of the linear diffusion process to ~~four~~ two first nonlinear transformation units in a succeeding encrypting section;

a key addition unit which adds key data of 128 bits to output data of 64 bits from the encrypting section of ~~the~~ a last stage,

wherein an encrypting section of [[a]] the last stage comprises two nonlinear transformation units each configured to perform a nonlinear transformation process for the first subblock data of 32 bits,

wherein each of the first nonlinear transformation units includes stage sections, each stage section including,

four second nonlinear transformation units each configured to perform a nonlinear transformation process for second subblock data of 8 bits which are obtained by dividing the first subblock data,

a second linear diffusion unit configured to perform a linear diffusion process for a group of the second subblock data of 32 bits output from the second nonlinear transformation units ~~with respect to the second size~~, and

an adder for adding a key to four second subblock data of 8 bits input to the four second nonlinear transformation units,

wherein a stage section of [[a]] the last stage comprises four second nonlinear transformation units each configured to perform a nonlinear transformation process for the second subblock data,

wherein the first nonlinear transformation units, the first linear diffusion unit, the second nonlinear transformation units, and the second linear diffusion unit are configured to connect at least one input bit terminal of the first nonlinear transformation units to one input bit terminal of the corresponding first nonlinear transformation units in the succeeding encrypting section via at least two paths, and

wherein each of the two first nonlinear transformation units divides input data of 32 bits into eight groups of data of 4 bits which are formed of extracting the input data by every

8 bits, and the first linear diffusion unit includes eight subunits each subunit receiving corresponding two groups of data of 4 bits output from the two first nonlinear transformation units, performing a 2 × 2 matrix operation based on multiplication over a Galois field GF(2^4) for the received two groups of data of 4 bits, and outputting two groups of data of 4 bits to corresponding two first nonlinear transformation units of the succeeding encrypting section.

14. (Currently Amended) A method for encrypting block data of a first size comprising:

randomizing each of first subblock data of a second size which are obtained by dividing the block data of the first size;

diffusing a group of the randomized data ~~with respect to the first size~~ of the first size; and

repeating the randomizing and the diffusing, wherein at least one bit input to the randomizing operation is ~~reflected on one bit input~~ transmitted to the next randomizing operation via at least two paths.

15. (Currently Amended) An article of manufacture comprising a computer readable medium including a computer program embodied therein, the computer program comprising:

computer readable program code means for causing a computer to randomize each of first subblock data of a second size which are obtained by dividing plaintext block data of a first size;

computer readable program code means for causing a computer to diffuse a group of the randomized data ~~with respect to the first size~~ of the first size; and

computer readable program code means for causing a computer to repeat the randomizing and the diffusing, wherein at least one bit input to the randomizing operation is ~~reflected on one bit input~~ transmitted to the next randomizing operation via at least two randomizing and diffusing paths.

16. (Currently Amended) An apparatus for decrypting encrypted block data comprising:

decrypting sections connected in series, each of the decrypting sections comprising,

first units each configured to randomize first subblock data of a second size which are obtained by dividing encrypted block data of the first size, and

a second unit configured to diffuse a group of data which is of the first size and is output from the first units ~~with respect to the first size~~ and supply a result of diffusion to first units in a succeeding encrypting section, and wherein the first units and the second unit are configured to connect at least one input bit terminal of the first units to one input bit terminal of the corresponding first unit in the succeeding encrypting section via at least two paths.

17. (Currently Amended) A method for decrypting encrypted block data of a first size, the method comprising:

randomizing first subblock data of a second size which are obtained by dividing the encrypted block data of the first size;

diffusing a group of the randomized data ~~with respect to the first size~~ of the first size; and

repeating the randomizing and the diffusing, wherein at least one bit input to the randomizing operation is ~~reflected on one bit input~~ transmitted to the next randomizing operation via at least two paths.

18. (Currently Amended) An article of manufacture comprising a computer readable medium including a computer program embodied therein, the computer program comprising:

computer readable program code means for causing a computer to randomize first subblock data of a second size which are obtained by dividing encrypted block data of a first size;

computer readable program code means for causing a computer to diffuse a group of the randomized data ~~with respect to the first size~~ of the first size; and

computer readable program code means for causing a computer to repeat the randomizing and the diffusing, wherein at least one bit input to the randomizing operation is ~~reflected on one bit input~~ transmitted to the next randomizing operation via at least two randomizing and diffusing paths.